



Cb Inspection User Guide

Product Version: 2016.3

Document Revised: 30 January 2018

Carbon Black, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@carbonblack.com
Web: <http://www.carbonblack.com>

Copyright © 2004-2018 Carbon Black, Inc. All rights reserved. This product may be covered under one or more patents pending. Carbon Black is a trademark of Carbon Black, Inc. in the United States and other countries. Any other trademarks and product names used herein may be the trademarks of their respective owners.

Contents

Overview.....	3
File Analysis with Cb Response	4
Requirement Summary	4
Modifying Cb Response for Cb Inspection Integration	4
Opting in to File Sharing for Cb Inspection	4
Analysis Workflow	7
Enabling the Feed for Analysis Results	7
Viewing Analysis Results in Cb Response.....	8
File Analysis with Cb Protection	9
Requirement Summary	9
Creating a Cb Inspection User in the Cb Protection Console.....	9
Installing the Cb Inspection Connector on the Cb Protection Server	11
Upgrade Installations.....	12
Viewing and Modifying the Connector Configuration.....	15
Analyzing Files	16
Viewing Analysis Results	19
Cb Protection Events for Cb Inspection	20
Using Event Rules for Automatic Analysis	21
Actions in Cb Protection Based on Analysis Results.....	23
Analysis Results on the Cb Inspection Console.....	24
Contacting Support.....	28
Reporting Problems	28

Overview

Cb Inspection (previously called “Cb Threat Intel File Analysis”) provides integrated analysis services from Carbon Black and its partners. Cb Response servers and Cb Protection (Bit9 Platform) Servers can send files from the endpoints they monitor to Cb Inspection for analysis. Once a file is analyzed, the analysis results are sent back to the server that requested them.

The analysis includes executing Windows 32-bit and 64-bit PE executables in a sandbox environment. Analysis results also include all of the metadata available for the file from the Carbon Black platform components that have seen it.

Cb Inspection is supported on:

- Cb Response versions 5.1.1 Patch 2 or later, and 5.2 or later
- Cb Protection (Bit9 Platform) versions 7.2.1 and 7.2.2 or later

For Cb Protection servers, you install a separate “connector” to enable use of Cb Inspection with a Cb Protection Server. The connector allows you to upload files, either by manually selecting each file or by creating *Event Rules* that automatically upload files matching your specifications. Once uploaded, files undergo static and dynamic analysis. Scoring information, along with details about observed behaviors, are returned via the connector, allowing you to examine any applicable telemetry from the service and drive policy based on results.

For Cb Response servers, Cb Inspection can be enabled through the existing console interface plus a configuration file change, and no additional installation is required. You must opt in to sending full binaries to both *Carbon Black & Alliance Partners* and to *3rd Party File Analysis*, which then allows files from sensor-monitored endpoints to be sent via the server to Cb Inspection for static and dynamic analysis. File scores and telemetry are returned to the Carbon Black server via a Threat Intelligence Feed and displayed in the console along with other data about the files sent. This information can then be used to drive detection and incident response use cases.

Cb Inspection provides visibility at the *endpoint*, greatly reducing the chances of missing a file that should be analyzed. In contrast, network detonation solutions might miss files encrypted in network traffic, files that arrive while an endpoint is outside the protected network perimeter, or files reaching an endpoint by out-of-band communications such as USB drives.

Caution: One potential consequence of dynamic analysis of files sent to this service is that an executable could make external network connections to arbitrary hosts and services on the Internet. For example, malware detonated by the service might connect to a malicious command and control server or a non-malicious executable might connect to a private entity on the Internet to download data. With an external connection by a file under analysis, it is possible that external parties, malicious or otherwise, could monitor traffic from that file. Although these connections would be initiated by the file on the Cb Inspection server, not your server, you should consider whether they could reveal proprietary information or expose the fact that analysis has occurred for a particular binary.

File Analysis with Cb Response

Requirement Summary

Use of Cb Inspection with Cb Response requires the following:

- You must have Cb Response 5.1.1 Patch 2 or later, or version 5.2 or later.
- For all versions of Cb Response, you must opt in to sending full binaries from your Cb Response server to *Carbon Black & Alliance Partners* and to *Cb Inspection* from one or more sensor groups.

Modifying Cb Response for Cb Inspection Integration

Cb Response 5.1.1 users must install Patch 2 or later on their server to use Cb Inspection. When you receive this patch, install it using the standard server patch installation instructions in the *Cb Response User Guide*.

In addition, use of Cb Inspection with Cb Response requires modification of the server's `cb.conf` file.

To configure `cb.conf` for Cb Inspection:

1. On the system running the Cb Response server (or the master server in a clustered environment) open the file `/etc/cb/cb.conf` for editing.
2. Add the setting `FeatureThirdPartySharing` and make its value `True`. You might also want to include a comment in the file so you know that this is for Cb Inspection. Be sure to follow the format guidelines for `cb.conf`, specifically keeping the parameter on its own line and not adding spaces:

```
# Add column to Sharing Settings page for Cb Inspection
FeatureThirdPartySharing=True
```

3. Save the file.
4. Restart Cb Response.
 - For a single server, run:
`service cb-enterprise restart`
 - For the master server in a cluster, run the following commands:
`/usr/share/cb/cbcluster stop`
`/usr/share/cb/cbcluster start`

Opting in to File Sharing for Cb Inspection

For all versions of Cb Response, use of Cb Inspection requires you to opt in to sending full binaries from your Cb Response server to both *Carbon Black & Alliance Partners* and *Cb Inspection* from one or more of the same sensor groups. See the *Cb Response User Guide* for complete details on Sharing Settings.

To opt in to 3rd Party File Analysis:

1. Log in to the Cb Response console using an account with Global administrator privileges.
2. On the console menu, choose **Administration > Sharing Settings**. The Sharing page appears.
3. Under General Sharing Settings, make sure the **Enable Alliance Communication** box is checked.
4. Scroll to the Endpoint Activity Sharing section at the bottom of the Sharing page.

Endpoint Activity Sharing

Some threat intelligence resources require your server to send endpoint activity to Carbon Black or our Alliance Partners. The threat intelligence databases may be too large or too dynamic to be hosted locally, analysis may be computationally intense or analysis may be dependent on external data sources. The activity sent varies with each dataset and terms of use with each partner. Complete details are available below.

	Carbon Black & Partners	Cb Inspection
Binary Hashes & Metadata	PARTIAL	N/A
Complete Binaries	DISABLED	DISABLED
Response Event Data	DISABLED	N/A

5. Ensure that you are sharing complete binaries from at least one sensor group in the column for Carbon Black & Alliance Partners. This means that in the *Complete Binaries* row, the *Carbon Black & Alliance Partners* column should read **Enabled** or **Partial**. Only sensor groups enabled for this column can also be enabled for Cb Inspection sharing. If the value shown is **Disabled**, click on that box and follow the instructions on the resulting page.

Note: See the *Cb Response User Guide* for full details about Sharing Settings.

6. In the *Complete Binaries* row, click on the value in the *Cb Inspection* column; the value will be **Disabled** if you have not enabled this feature before. This opens the *Share binaries with Cb Inspection* page. This page describes the data that will be shared, and it provides a privacy statement to review.

✕

Share binaries with Cb Inspection

Summary

Sharing binaries with Cb Inspection allows dynamic and static analyses to be performed by both Carbon Black and third parties, with verdict and result information returned as part of the Cb Inspection feature. The nature of these services require that full binaries be sent outside of the Carbon Black infrastructure for processing within 3rd party partner infrastructures. These partners may retain binaries and analysis information related to those binaries, but will not as a practice disclose those binaries or direct analyses to other customers or the general public. Binaries may be stored and analyzed in Partner infrastructures in the United States, Europe, and other countries or jurisdictions outside your own, where data standards may be different.

Data Shared

Every binary executed in the groups below will be analyzed by Carbon Black and uploaded to 3rd Party Partners for analysis.

Raw file contents for any executable under 25MB.

Privacy

- Partners may retain binaries and analysis information related to those binaries, but will not as a practice disclose those binaries or direct analyses to other customers or the general public.
- Binaries may be stored and analyzed in Partner infrastructures in the United States, Europe, and other countries or jurisdictions outside your own, where data standards may be different.

[Click here to view the EULA.](https://www.carbonblack.com/license-agreements/carbon-black-threat-intel-file-analysis-license-agreement/)
<https://www.carbonblack.com/license-agreements/carbon-black-threat-intel-file-analysis-license-agreement/>

7. Review all of the sharing and privacy information carefully, including the linked EULA, before making sharing choices. The full EULA is also available through your browser at: <https://www.carbonblack.com/license-agreements/carbon-black-threat-intel-file-analysis-license-agreement/>
8. If you agree to share this data, go to the bottom of the page and do one of the following:
 - a. Click **Enable** to share data from endpoints in all Sensor Groups.
 - b. Click **Partial** to share data from endpoints in some Sensor Groups, and use the arrow between the SHARE FROM and DO NOT SHARE FROM windows to choose which groups you will allow to share data.

Note: A sensor group must first have binary sharing with *Carbon Black & Alliance Partners* enabled (as described in Step 5) before it can be enabled to share Complete Binaries with *Cb Inspection*.

ENABLE (Share from ALL Groups)

DISABLE (Do Not Share from ANY Groups)

PARTIAL (Share from SOME Groups)

SHARE FROM

Default Group

DO NOT SHARE FROM

R&D

Close Share

9. When you have finished making your sharing choices, click the **Share** button.

Analysis Workflow

Once you enable Cb Inspection, any binaries that are executed on your Cb Response endpoints will be sent for both static and dynamic analysis. This includes executing Windows 32-bit and 64-bit PE executables in a sandbox environment.

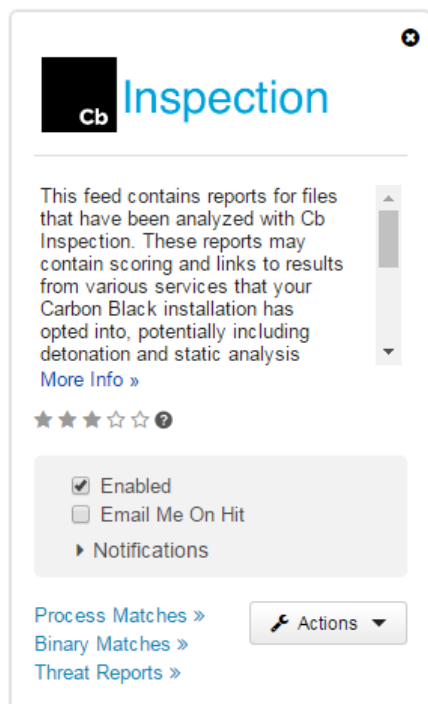
Caution: One potential consequence of dynamic analysis of files sent to this service is that an executable could make external network connections to arbitrary hosts and services on the Internet. For example, malware detonated by the service might connect to a malicious command and control server. Another example would be a non-malicious executable connecting to a private entity on the Internet to download data. With an external connection by a file under analysis, there is the possibility that external parties, malicious or otherwise, could monitor traffic from that file. Although these connections would be initiated by the file on the Cb Inspection server, not your server, you should consider whether they could reveal proprietary information or expose the fact that analysis has occurred for a particular binary.

Enabling the Feed for Analysis Results

To receive the results from files sent to Cb Inspection, you enable the File Analysis feed. This feed reports scores and telemetry only for the files uploaded to the Cb Alliance from your site, not results from other customers' submissions. The feed reports have a score per hash, which is displayed throughout the Cb Response user interface in the same way as data from other feeds. You must enable the feed to get file analysis results.

To enable the Cb Inspection Feed:

1. Log in to the Cb Response console using an account with Global administrator privileges.
2. On the console menu, choose **Detect > Threat Intelligence**. The Threat Intelligence Feeds page appears.
3. On the Cb Inspection feed panel, click **Enabled** and configure any of the other options, such as Notifications, that you choose.



Viewing Analysis Results in Cb Response

Results from this feed for a particular file may be viewed in the same way as those from other feeds, for example, on the Binary Analysis page. If you want to view all results from the feed, you can use the Process Matches, Binary Matches, and Threat Reports links on the feed panel.

As with other feeds, you can set up a Watchlist or Alert for results from the feed.

In addition to data that displays directly in the Cb Response console, Feed Reports from Cb Inspection also include a link to the Cb Collective Defense Cloud, which shows further results of the analysis. See [Analysis Results on the Cb Inspection Console](#) on page 24 for a sample of the results provided there.

See the *Cb Response User Guide* for full information about using feeds, creating watchlists, viewing feed data on the Binary and Process pages, and response options when a malicious file is reported.

File Analysis with Cb Protection

Requirement Summary

- The Cb Protection (Bit9 Platform) Server must be at version 7.2.1 or greater. In addition, files can be uploaded only from agents at version 7.0.0 or greater.
- The Cb Protection Server license must include File Upload capabilities.
- You must obtain an activation token for Cb Inspection. If you have multiple Cb Protection Servers, you must obtain one token for each.
- An internet connection is required for installing and using the connector. In addition, the server must be able to communicate with threatintel.bit9.com on port 443; this is outbound only.
- Before installing the connector, you must add a Cb Protection Console user for actions taken by this connector.
- You must download and install the Connector for Cb Inspection on your Cb Protection Server, providing the configuration information described in this document. During connector installation, you also must accept the license agreement, which allows Carbon Black to authorize your access to the Cb Inspection service.

Creating a Cb Inspection User in the Cb Protection Console

Before installing the connector, you must add a Cb Protection Console user for actions taken by this connector. An API token for this user is used in the connector installation.

Note: The steps and screenshots shown here are for Bit9 Platform v7.2.3. The procedure for Cb Protection v8.0.0 is very similar, with variations due to changes in the Login Accounts interface.

To create a connector user account in the Cb Protection Console:

1. Log in to the Cb Protection Console using an administrative account.
2. From the console menu, choose **Administration > Login Accounts**.
3. Click the **Groups** tab.

Name	Status	AD Rank	AD Mapping	Date Modified	User Count
Administrator	Enabled	1	Bit9 Administrators	Oct 25 2011 04:08:33PM	3
PowerUser	Enabled	3	Bit9 Power Users	Oct 14 2011 08:49:49AM	6
ReadOnly	Enabled	4	Bit9 Readonly Users	Oct 14 2011 08:49:49AM	20
Unauthorized	Enabled	5		Oct 26 2011 10:30:22AM	62

For the connector user, you must have a group with the following permissions:

- View Files
- View File Uploads
- Submit Files For Analysis
- View System Configuration
- Extend Connectors Through API

Since connector users are not generally used to log in to the console, it is a good idea to limit permissions to just those needed. You can modify an existing group for this purpose, but a better option is to create a new group specifically for connectors.

4. If you choose to create a dedicated Connectors group, on the Login Accounts page, click the **Add Group** button on the Groups tab and provide the following configuration:
 - a. Give the group an appropriate group name for its purpose, for example, *Connectors*.
 - b. Click the **Enable** radio button.
 - c. Check the boxes for the permissions listed above.
 - d. When you finish configuring the group, click **Save** at the bottom of the page.

Add Group ?

General

Name:

Description:

Status: Enabled Disabled

Permissions

Asset	Permission	<input type="checkbox"/> Enabled
Computers	View computers	<input type="checkbox"/>
Computers	Temporary assign computers	<input type="checkbox"/>
Computers	Manage computers	<input type="checkbox"/>
Computers	Change advanced options	<input type="checkbox"/>
Files	View files	<input checked="" type="checkbox"/>
Files	Manage files	<input type="checkbox"/>
Tools	View file uploads	<input checked="" type="checkbox"/>
Tools	Manage uploads of inventoried files	<input type="checkbox"/>
Tools	Manage uploads of files by pathname	<input type="checkbox"/>
Tools	Access uploaded files	<input type="checkbox"/>
Tools	Submit files for analysis	<input checked="" type="checkbox"/>
Notifiers	View notifiers	<input type="checkbox"/>
Notifiers	Manage notifiers	<input type="checkbox"/>
Analytics	View external analytics reports	<input type="checkbox"/>
Administration	View system configuration	<input checked="" type="checkbox"/>
Administration	Manage system configuration	<input type="checkbox"/>
Administration	View login accounts and groups	<input type="checkbox"/>
Administration	Manage login accounts	<input type="checkbox"/>
Administration	Manage groups	<input type="checkbox"/>
Administration	View System Health Indicators	<input type="checkbox"/>
Administration	Extend connectors through API	<input checked="" type="checkbox"/>

5. You should not map this group via AD mapping – as noted above, the account you create in this group is only for validating the Connector integration with the Cb Protection

Server, not for logging in as a user. However, if you are unable to prevent AD mapping of this group, be sure to lower the rank of the mapping rank so that it does prevent mapping of users to other Cb Protection groups with greater privileges.

6. On the Login Accounts page, click the **Users** tab and then click the **Add User** button.
7. On the Add User page, create a user with a name that clearly identifies it as the user for this connector, for example, *CbInspection*. Provide the following information for the user and click **Add User** when finished:
 - a. Enter the User Name.
 - b. Enter the Password and confirmation
 - c. Choose the group with the correct permissions from the Group menu.
 - d. (optional) Add a Comment describing the purpose of this user.

8. Once you have created the Cb Inspection user account, create an API key for that user.
 - a. If you are not still on the Add/Edit Login Account screen for the user, choose **Administration > Login Accounts**.
 - b. On the **Users** tab click the View Details icon (📄) for the user.
 - c. On the Edit Login Account screen, click on the **Show API token** checkbox.

- d. If no API token is shown, click on the **Generate** button to create one.
- e. Click **Save** at the bottom of the screen. You will return to this page later, during the Connector installation.

Installing the Cb Inspection Connector on the Cb Protection Server

The Cb Inspection connector may be installed on Cb Protection Server versions 7.2.1 and greater, licensed for File Uploads. An internet connection is required during installation. You also will need the email you received when you arranged to add this service. It contains a download link for the installer and the activation key used for the connector.

The connector is a Windows service that runs under the Local System account by default.

Program Files for the connector are located by default in the following folder:

```
<CbProtectionServerInstallationFolder>\Integrations\CbInspection
```

By default, the Cb Protection Server installation directory is `c:\Program Files (x86)\Bit9`.

Log files for the connector are located in the following folder:

`%PROGRAMDATA%\Carbon Black\Cb Inspection\Logs`

Upgrade Installations

If you have installed previous versions of the connector (versions 2.1.0 and earlier), you must uninstall the earlier version before you install the new version. This will uninstall the program but leave your credentials in place.

The name of the file analysis service has changed to “Cb Inspection” from its previous name. During installation of this release on a system that had a previous release installed, the following changes will be made:

- The installer will move your credentials from the “CarbonBlackThreatIntelFileAnalysis” folder to a new “CbInspection” folder in the Cb Protection Server installation folder. This eliminates the extra step of having you enter your credentials again during the new installation.
- When installation of this version is successfully completed, the “CarbonBlackThreatIntelFileAnlysis” folder will be removed.
- The previous connector (under its previous name) will be removed from the list of connectors you see on the Connectors tab of the System Configuration page in the Cb Protection Console; for this version, the tab should read “Cb Inspection”.

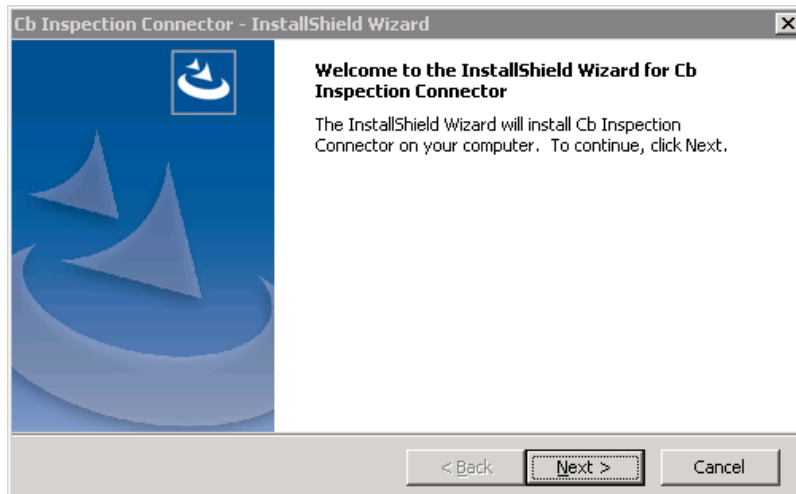
Also note that the earliest pre-release versions of the connector were based on Python; this version does not require or use Python.

To install the Cb Inspection connector on a Cb Protection Server:

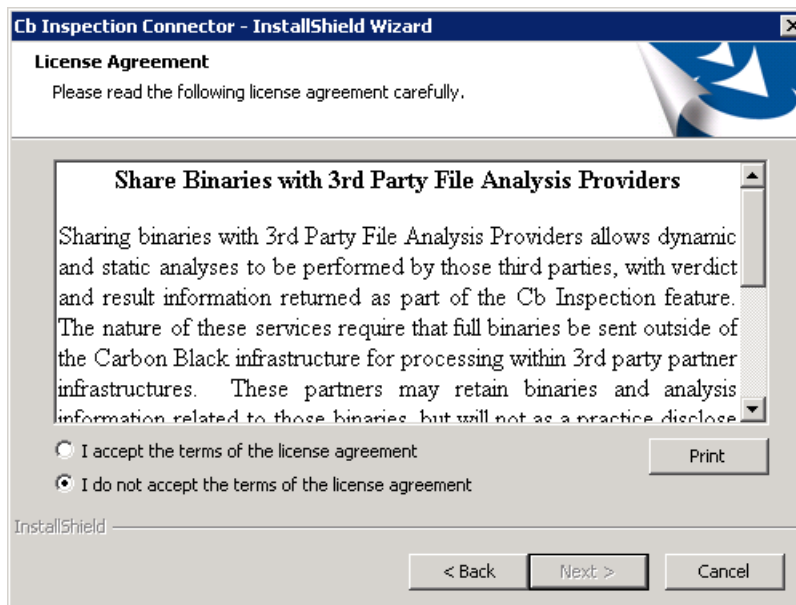
1. Log in to the server using a Windows account with administrator privileges.
2. If you installed a previous version of the Cb Inspection connector, go to the Windows Control Panel and uninstall it. If you used an early connector version that required Python and you are not using Python for any other purpose, you can also uninstall it.
3. Download the Cb Inspection installer, **CarbonBlackInspectionConnector-v2.2.0-Setup.exe**, to your server.

Note: You may receive different releases in the future, in which case the “v2.2.0” portion of the filename may change to reflect the version of the new release.

4. As a user with administrative privileges, run the installer (double-click the icon, use Run, or run in a command window). The Welcome page appears.



5. Click **Next**. The License Agreement page appears. On the License Agreement page, you can read the agreement in the dialog box or click Print to print or download it to your server for easier reading.



To access the full terms and End User License Agreement for Cb Inspection, please visit <https://www.carbonblack.com/license-agreements/carbon-black-threat-intel-file-analysis-license-agreement>.

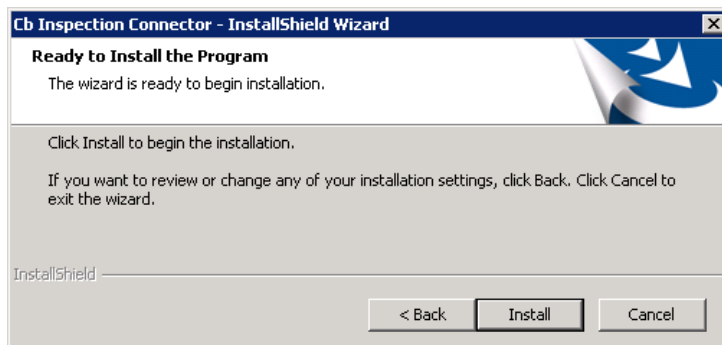
6. If you accept the terms, click the “I accept...” radio button and then click **Next**. If you have never installed any version of the connector before, the next dialog requests information to establish the connection between your server and Cb Inspection.

Note: If had a previous version of the Connector installed, your credentials will have been saved, and if they are still valid, you will not see the next screen, skipping instead to the Ready to Install screen (step 8).

7. Provide the following information in the requested information dialog:
 - a. **Cb Protection server URI** – This is the server name for the Cb Protection Server on which you are installing this connector. This must be a FQDN. Numeric IP addresses will fail the certificate check at this stage.
 - b. **Cb Protection server API token** – This is the API token for the special Cb Protection Console user you created. To see the API token, in the Cb Protection Console, navigate to the **Administration > Login Accounts** page, click the **Details** button for the Cb Inspection user you created (e.g., *CbInspection*), and scroll to the bottom of the page. Click on Show API token. If there is no token, click the **Generate** button. Copy the resulting string into the field in the install dialog.

- c. **Cb Collective Defense Cloud activation token** – This is the token supplied via email when you purchased this connector.

Note: If any of the information you enter here is found not to be valid, you will be re-prompted to correct the invalid information.
8. When you have provided all of this information, click **Next**. The Ready to Install the Program dialog appears.



9. Click **Install**. The Installation begins.

The information you provide is checked against your server and records of your activation token. If any of it is inaccurate or missing, an error message appears. Otherwise, the InstallShield Wizard Complete dialog appears.



10. Click **Finish**. Once installed, the connector is enabled on the Cb Protection Server.

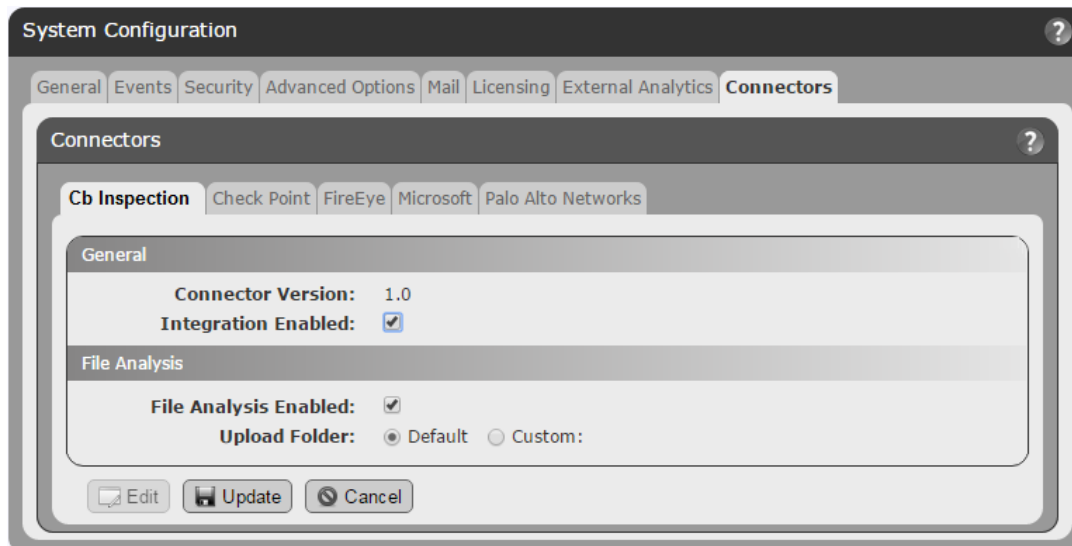
Viewing and Modifying the Connector Configuration

The Cb Inspection Connector configuration is shown on the Connectors tab of the Cb Protection Console System Configuration page. There, you can do the following:

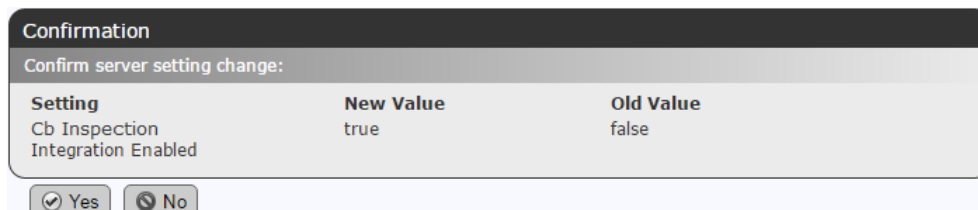
- View the version of the currently installed Connector
- Disable and then re-enable the Connector (note that the Cb Inspection Connector is enabled automatically at the end of its installation)
- Change the location on the server to which agent files are uploaded

To view and modify the Cb Inspection connector configuration for Cb Protection:

1. In the Cb Protection Console, choose **Administration > System Configuration** from the console menu, and on the System Configuration page, click the **Connectors** tab and then click on the **Cb Inspection** tab. The installed Connector Version is shown on this tab.



2. Click the **Edit** button at the bottom of the page to change the settings.
3. If you want to disable the connector, uncheck the **Integration Enabled** box.
4. If you want to re-enable a disabled connector, check the **Integration Enabled** box. The **File Analysis Enabled** box should be checked by default, but if it is not, also check it.
5. If you want to upload files from agents to a different server folder than the default, click the **Custom** radio button and provide that path. The default upload location for analysis files can be viewed on the Advanced Options tab of the System Administration page. It is usually *Parity Server\files* under the Cb Protection installation directory.
6. When you have finished configuring the connector, click **Update**. A confirmation dialog appears. For example, if you re-enabled the connector, you would see this:



7. Click **Yes** to confirm that you want to accept the changes.

Analyzing Files

Once the connector is activated, you can analyze files that are inventoried on your Cb Protection Server. This can be done in most locations in which files are listed in tables, including the Events page (for events that include a file). It can also be done from the File Details page for one file. See “Analysis of Suspicious Files on Endpoints” in *Using Cb Protection* or the online console Help for more details about where you can initiate file analysis and how files are processed for upload.

You can also create Event Rules that automate upload of certain files for analysis. This is described in [Using Event Rules for Automatic Analysis](#) on page 21.

Caution: One potential consequence of dynamic analysis of files sent to this service is that an executable could make external network connections to arbitrary hosts and services on the Internet. For example, malware detonated by the service might connect to a malicious command and control server. Another example would be a non-malicious executable connecting to a private entity on the Internet to download data. With an external connection by a file under analysis, there is the possibility that external parties, malicious or otherwise, could monitor traffic from that file. Although these connections would be initiated by the file on the Cb Inspection server, not your server, you should consider whether they could reveal proprietary information or expose the fact that analysis has occurred for a particular binary.

When analysis is complete, scores and telemetry are sent back via the connector. At the site that sent the file for analysis, a score can drive policy and alerting for Cb Protection, and there will be a link from the results back to the analysis details on the Cb Predictive Security Cloud. Scoring information from detonation will affect trust and threat scoring in the Cb Predictive Security Cloud within a few hours.

To send one or more files to Cb Inspection:

1. Navigate to a Cb Protection Console page that list files.
2. Check the box(es) next to the file(s) you want to analyze.

Files: All Unique Files

File Catalog | Files on Computers

Saved Views: (The Current View Has Unsaved Changes - Discard) (none) Add

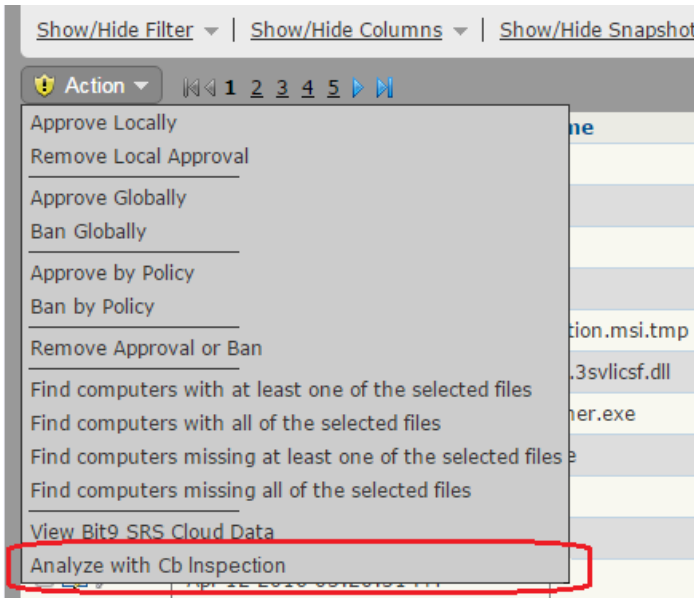
Group By: (none) Ascending

Show/Hide Filter | Show/Hide Columns | Show/Hide Snapshot | Export to CSV | Refresh Page

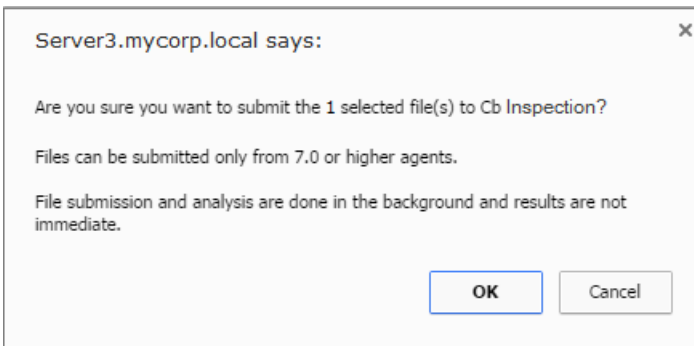
Action

	First Seen Date	First Seen Name	Publisher or Company
<input type="checkbox"/>	Apr 12 2016 02:19:39 PM	issetup.dll	Flexera Software LLC
<input type="checkbox"/>	Apr 12 2016 02:19:46 PM	notepad++.exe	Don HO don.h@free.fr
<input checked="" type="checkbox"/>	Apr 12 2016 02:19:46 PM	curl.exe	cURL, http://curl.haxx.se/
<input type="checkbox"/>	Apr 12 2016 02:19:46 PM	libeay32.dll	The OpenSSL Project, http://www.openssl.org/

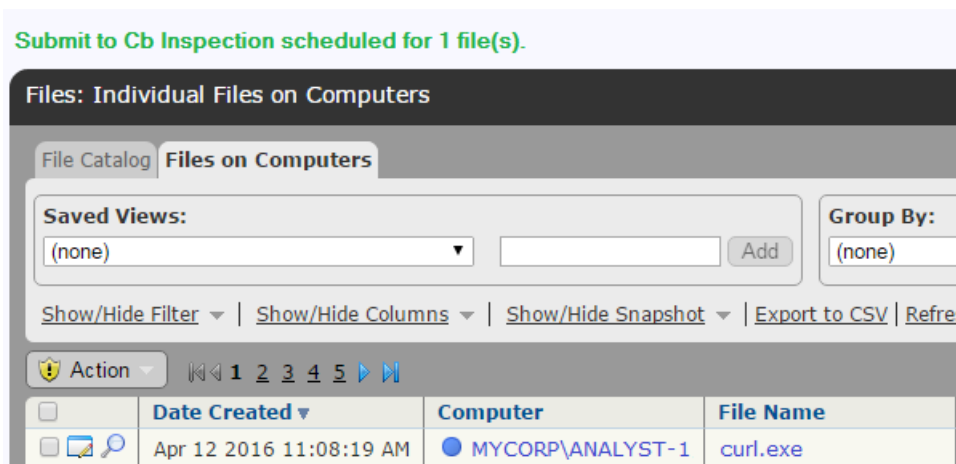
3. On the Action menu, choose **Analyze with Cb Inspection**.



4. Confirm the file submission.



When you submit the file(s) successfully, a message appears at the top of the page from which they were sent.



To send one file for analysis from the File Details page:

- On the File Details page, click on **Analyze with...** in the Advanced menu, choose **Cb Inspection**, and confirm your choice.

The screenshot shows the 'File Properties' section on the left with the following details:

- Publisher:** (none)
- Company:** cURL, http://curl.haxx.se/
- Product Name:** The cURL executable
- Product Version:** 7.39.0
- File Size:** 619,008 bytes

On the right, the 'Advanced' menu is open, showing 'View Bit9 SRS Data' and 'Analyze with...'. A dropdown menu is displayed below it, with 'Cb Inspection Analysis' and 'Cb Inspection' as options.

From this page, you can click the **Analysis Submissions** link in the Related Views menu to see the results specifically for this file.

Viewing Analysis Results

Once files are sent for analysis, you can monitor them in the console by going to **Tools > Requested Files** and clicking on the **Analyzed Files** tab.

The screenshot shows the 'Requested Files: Analyzed Files' page. It has tabs for 'Uploaded Files', 'Analyzed Files', and 'Diagnostic Files'. Below the tabs are 'Saved Views' and 'Group By' sections. The main table has the following columns: Request Date, Priority, Requester, Status, Target, and Analysis Result. One row is visible with the following data:

Request Date	Priority	Requester	Status	Target	Analysis Result
Apr 12 2016 03:03:55 PM	High	admin	Analyzing	Cb Inspection	

The Status field will tell you initially that the file status is *Uploading* or *Analyzing*, and will indicate any error conditions. Once results are available, they will be displayed in the Analysis Result field for each file. Note that you might need to click the **Refresh Page** link to display the results if you have not navigated away from the page.

The screenshot shows the 'Requested Files: Analyzed Files' page after a refresh. The table now shows the following data:

Request Date	Requester	Status	Target	Analysis Result	File Name
Apr 12 2016 03:17:55 PM	admin	Analyzed	Cb Inspection	Clean	curl.exe

At the bottom of the page, it indicates '1 item' and 'Page 1/1'.

When results come back, clicking on the **Analyzed** link in Status opens the External Notification Details page for the analysis. This provides more details about the analysis.

External Notification Details ?

Cb Inspection Details

Type: clean_file

Malicious: no

Severity: low

Product: Cb Inspection

Time: Apr 14 2016 06:45:56 PM

Bit9 Details

Received Time: Apr 14 2016 06:45:56 PM

Status: Notified

Comment:

Total Files (1)
Known Files (1)
Files On Computers (1)
History

Saved Views: (none) Add

Group By: (none) Ascending

[Show/Hide Filter](#) | [Show/Hide Columns](#) | [Export to CSV](#) | [Refresh Page](#)

Action

	Sequence	Operation	File Name	Size	MD5
<input type="checkbox"/>	1	created	notepad+ .exe	2318848	18365B3D9C3ADE5EE8ECD36791EE57C8

1 item Page 1/1 25 rows per page

Update Cancel

Related Views

[Bit9 Computer](#)

Actions

[Escalate Notification](#)

[Resolve Notification](#)

[Close Notification](#)

External Pages

[Cb Inspection Console](#)

See *Using Cb Protection* or the online console Help for more about the information available in an External Notification Details page.

To see the full results of a Cb Inspection, click the **Cb Inspection Console** link in the External Pages menu on the External Notification Details page. The section [Analysis Results on the Cb Inspection Console](#) later in this document describes the information available there.

Cb Protection Events for Cb Inspection

There are Cb Protection events related to Cb Inspection, including for the file analysis itself and for the installation and activation of the connector. Choosing the Saved View *Connectors* on the Events page will show these events (along with events related to any other connectors you have installed), or you can use other filters to narrow down your results. The following shows some of these events.

Timestamp	Severity	Type	Subtype	Source	Description
Apr 12 2016 03:17:55 PM	Info	Server Management	File analysis requested	MYCORP\ANALYST-1	User 'admin' requested analysis of file 'msgviewerlite.exe' [F0081...177E7] with 'Cb Inspection'.
Apr 12 2016 03:17:55 PM	Info	Server Management	File analysis requested	MYCORP\ANALYST-1	User 'admin' requested analysis of file 'bantest1234.bat' [74DCA...37803] with 'Cb Inspection'.
Apr 12 2016 03:02:34 PM	Info	Server Management	Network Connector	System	User 'admin' has enabled Network Connector 'Cb Inspection'.
Apr 12 2016 03:00:23 PM	Notice	Server Management	Network Connector added	System	User 'Cb Inspection' registered new Network Connector 'Cb Inspection', version '1.0'.
Apr 12 2016 02:58:01 PM	Notice	Session Management	Console user modified	System	'admin' created the API token for 'Cb Inspection'.
Apr 12 2016 02:57:33 PM	Info	Session Management	Console user created	System	'admin' created new username 'Cb Inspection'.

Using Event Rules for Automatic Analysis

Event Rules allow you to specify an action to be performed when a file- or computer-related event occurs that matches filters you define. To use this feature, a console user must have *Manage event rules* permission. If you would like to automatically analyze certain files in your environment, you can create an Event Rule to initiate the analysis based on a wide variety of criteria. One way to create such a rule is to begin with a sample rule already on your server.

There is a sample Event Rule called “[Sample] Analyze downloaded files.” This rule will send any file downloaded from a web browser to an agent-managed computer for analysis. You can modify this sample rule to automate analysis with the Cb Inspection service.

To use an Event Rule to automatically upload files to Cb Inspection:

1. In the Cb Protection Console, choose **Rules > Event Rules**, and on the Event Rules page, click **Create Rule**.
2. On the Create Event Rule page, select **[Sample] Analyze downloaded files** from the *Copy Settings From* drop-down menu.

Create Event Rule

General

Copy Settings From: (none)

Rule Name: (none)

Description: [Sample] Analyze files from approval requests
[Sample] Resolve approval requests for clean files
[Sample] Analyze downloaded files
[Sample] Report Malicious files

Status: Enabled Simulate only Disabled

3. Change the Rule Name to “Analyze downloaded files with Cb Inspection.”
4. Change the Description to indicate that you are using Cb Inspection.
5. Leave the filters in Select Event Properties panel as configured.

6. Modify the filters in the Select File Properties panel:
 - a. Delete the filter item “Analysis Result: Palo Alto Networks Wildfire”.
 - b. On the Add filter menu, choose **Analysis Result: Cb Inspection** with the values of **is** and **Unknown**.
7. In the Select Action panel, check the box for **Use Cb Inspection**.
8. In the status line in the top panel, click the **Simulate only** radio button. When the rule is configured, the values match those in the screen below (changed circled in red here).

Create Event Rule

General

Copy Settings From: (none)

Rule Name: Analyze downloaded files with Cb Inspection

Description: Automatically analyze all files downloaded from web browsers with Cb Inspection

Status: Enabled Simulate only Disabled

Select Event Properties

Add filter

File Name doesn't contain .crdownload

or .part

Process ends with iexplore.exe

or firefox.exe

or chrome.exe

Subtype is New file on network

Select File Properties

Add filter

Analysis Result: Cb Inspection is Unknown

File Size smaller than 25000000

File State is not Approved

File Type is Application

Select Process Properties

Add filter

Select Action

Action: Analyze file

Priority: Medium

Use Cb Inspection:

Create & Exit Save Cancel

Important: Use of *Simulate only* is always recommended before fully enabling an Event Rule that can take an action that could have significant impact, such as sending a large number of files for analysis. Once you have seen what the impact *would* be, you can change the rule status to **Enabled**.

9. When the rule is configured, click **Create & Exit**.

Once this rule is activated in Simulate only mode, any event processed because of this rule appears in a Processed Events panel at the bottom of the details page for the event rule. You can monitor the volume of files that *would have* been sent for analysis over a given period, and if you are satisfied that you will not be sending too many events, change the rule status to **Enabled**.

When the rule is fully enabled, any files matching the settings are sent to Cb Inspection automatically. You can view any results on the Requested Files page as described above in the “Manual Analysis” section.

See the *Using Cb Protection* guide or the online help in the Cb Protection Console for more about creating Event Rules.

Actions in Cb Protection Based on Analysis Results

Once an analysis is completed, you can respond to interesting results by taking manual or automated actions. For example, you could manually ban a file that returns Cb Inspection results that suggest a threat, or manually approve a file that comes back with clean results. You might also consider using one of the other ban or approval methods, such as putting files that come back as “clean” into a Trusted Directory.

A variety of automated actions based on analysis results can be taken using Event Rules. For example, you can automatically create a “Report ban” for files reported as malicious. Report bans do not prevent a file from running but let you know when a file would have been banned had the ban been fully enabled. You can enable one of the sample rules to create these report bans when *any source* reports a malicious file or make a rule specific to Cb Inspection results.

Note: Banning files via Event Rules is not enabled in the default Cb Protection interface. If you want to create active bans (not “Report only”) with Event Rules, contact Carbon Black Support.

To create a “Report ban” for malicious files reported by Cb Inspection:

1. In the Cb Protection Console, choose **Rules > Event Rules**, and on the Event Rules page, click **Create Rule**.
2. On the Create Event Rule page, select **[Sample] Report Malicious files** from the *Copy Settings From* drop-down menu.
3. Change the *Rule Name* to “Ban Malicious files reported by Cb Inspection.”
4. Leave the filters in Select Event Properties as configured.
5. In the Select File Properties panel, choose **Analysis Result: Cb Inspection** from the Add Filters menu and choose **is** and **Malicious** for its values.
6. In the Select Action panel, choose **Change global file state** on the *Action* menu.
7. In the Change Global State field, click the **Ban (Report only)** radio button.
8. Leave the *Resolve Related Approval Request* box unchecked.
9. In the *Create for* field, click the **All policies** radio button.
10. In the *General* panel, set the Status of the rule to **Enabled**, then click **Create & Exit** at the bottom of the page.

Note: Because this is a report-only rule, it is not necessary to run it in Simulate mode to start with. However, if you create an active ban, testing it first in Simulate mode is recommended.

Analysis Results on the Cb Inspection Console

In addition to the analysis details displayed in the Cb Response or Cb Protection Console, you can go directly to the Cb Inspection Console to see detailed results of the analysis performed when you send a file for analysis.

CARBON
BLACK Cb Inspection
ARM YOUR ENDPOINTS

Overview MD5 6c8d28d1cc0f20b1998608859c4011c6

Metadata SHA256 7f853fda3449e7814d3c48d816a7cd6e9d15b78f95122fbc017879a6aa080613

Detonation Results File Description verybadthings

Strings Analysis

Back to top

100

Analysis Score **Malicious**

Overview

Dynamic Analysis Verdict	100 Malicious details ...
CB Reputation	0 ■■■■■■■■■■ Low trust
Malware Signature	Trojan.Win32.Generic.W.gnudu
Malware Family	Strictor
Signature	This binary is not signed details ...
Last Analyzed	May 20, 2016
First Seen	May 19, 2016

Metadata





File Type	PE32 executable for MS Windows (GUI) Intel 80386 Mono/.Net assembly
Original File Name	6C8D28D1CC0F20B1998608859C4011C6.zip
Signature	This binary is not signed
File Hashes	MD5 6c8d28d1cc0f20b1998608859c4011c6 SHA1 a6296a52ebfc6f160d14cd6ceca95aba5e11ef50 SHA256 7f853fda3449e7814d3c48d816a7cd6e9d15b78f95122fbc017879a

Results in Cb Inspection vary depending upon whether a submitted file is found to be malicious and also on the information available for it from Carbon Black and other sources. The Binary Analysis page on the portal includes the following sections:

- The top of the page is a quick summary of the analysis, with the MD5 and SHA256 hashes for the file, the file description, the analysis score and the analysis verdict.
- **Overview** – This summarizes analysis data for the file, including the Cb Inspection analysis verdict, Cb Reputation data, the malware signature and family, the signature on the file, when it was last analyzed and when it was first seen. Not all files will have all of this data.


- **Metadata** – This summarizes the metadata for the file available in the file inventories of Cb Response and Cb Protection. It can include the file hashes (MD5, SHA1 and SHA256), original file name, file size, file type, certificates, file description, product name, product version, company, copyright, and icons.

Metadata

File Type	PE32 executable for MS Windows (GUI) Intel 80386 Mono/.Net assembly
Original File Name	6C8D28D1CC0F20B1998608859C4011C6.zip
Signature	 This binary is not signed
File Hashes	MD5 6c8d28d1cc0f20b1998608859c4011c6  SHA1 a6296a52ebfc6f160d14cd6ceca95aba5e11ef50  SHA256 7f853fda3449e7814d3c48d816a7cd6e9d15b78f95122fbc017879a6aa080613 
File Description	verybadthings
File Version	1.0.0.0
Product Name	verybadthings
Product Version	1.0.0.0

- **Detonation Results** – This is the report from one or more third-party detonation providers partnering with Carbon Black.

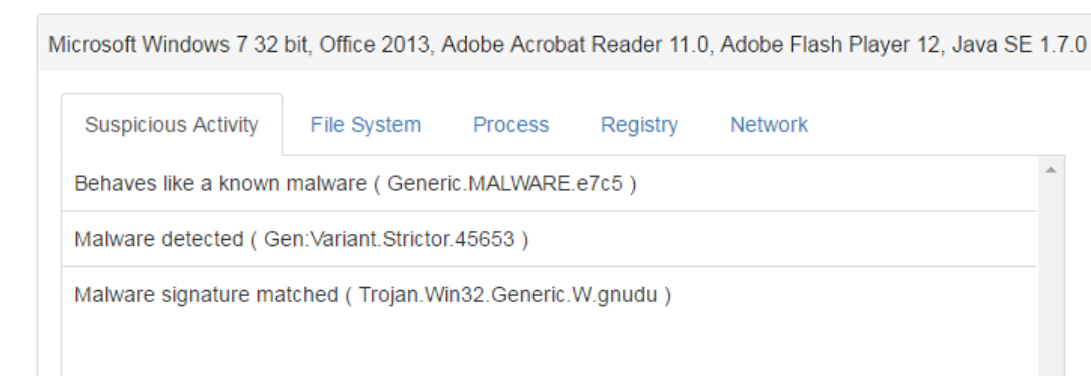
Detonation Results

Detonated	May 20, 2016
Assessment	 Malicious
Score	100
Antivirus Signature	Trojan.Win32.Generic.W.gnudu
Outbound IP addresses	169.254.0.69, 169.254.0.85, 169.254.0.65, 169.254.0.81, 169.254.0.93
Outbound Domains	www.mp3search.ru

- **Detonated** – Date of detonation.
- **Assessment** – The results of the detonation. The value can be *Malicious*, *Suspicious*, or *No signs of malware*.
- **Score** – This ranges from 0 (good) to 100 (bad).
- **Antivirus signature** – This field shows the antivirus signature, if any, provided for this file in the records of one or more third-party partners. It can give a brief description about the type of malware which was identified.

- **Outbound IP addresses** – This field shows the outbound IP addresses the malware attempted to connect to, if any.
- **Outbound Domains** – This field shows the outbound domains the malware attempted to connect to, if any.
- **Detonation Details** – This shows the detailed output of a detonation and a description of the detonation environment. If the score is 0 (good), this section will be blank. For a file with a non-zero score, the results are organized into boxes representing different detonation environments. The detonation environment is described at the top of the box, and includes the operating system and any significant application software that might interact with malware.

Detonation Details



You can click on tabs in each box within Detonation Details to see different types of data (if available; not all tabs will have data):

- Suspicious Activity
- File System
- Process
- Registry
- Network
- **Yara** – Cb Inspection runs YARA signatures against files submitted for analysis. These YARA signatures are maintained by the Carbon Black Threat Research Team, and hits contribute to the overall score for a particular analyzed file. See <http://virustotal.github.io/yara/> for more information about YARA.

Yara

Rule	Severity	Confidence	Description
ms15_093_plugx_dll_payload	5	5	Found a specific plugx variant DLL payload, https://blog.bit9.com/2015/09/04/threat-research-team-goes-beyond-the-exploit-in-search-of-payloads-from-ms15-093/
ms15_093_plugx_dropper	4	4	Found a specific plugx variant dropper.
suspicious_strings	0	4	Suspicious strings identified.

- **Strings Analysis** – This has two boxes, showing the Unicode and ASCII strings found in the analyzed file. In the ASCII box, strings that are in bold show system calls. The highlighted system calls do not necessarily indicate that the file contains or is malware, but they are often found within malware samples.

Strings Analysis

Unicode Strings

```

#+3;CScs
MS Shell Dlg
MS Shell Dlg
msctls_progress32
SysListView32
MS Shell Dlg
Please wait while Setup is loading...

```

ASCII Strings

```

OpenProcessToken
RegDeleteKeyA
RegDeleteValueA
RegCloseKey
RegEnumKeyA
ShellExecuteA
PeekMessageA
GetMessagePos
SetTimer

```

Contacting Support

For your convenience, Carbon Black Technical Support offers several channels for resolving support questions:

Technical Support Contact Options
Web: Carbon Black User eXchange
E-mail: support@carbonblack.com
Phone: 877.248.9098
Fax: 617.393.7499

Reporting Problems

When you call or e-mail technical support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and email address
Product version	Product name and version number
Hardware configuration	Hardware configuration of the server or computer the product is running on (processor, memory, and RAM)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear on the cover page, or for longer manuals, after the Copyrights and Notices section of the manual.
Problem	Action causing the problem, error message returned, and any other appropriate output
Problem severity	Critical, serious, minor, or enhancement